AO 106 (Rev. 04/10) Application for a Search Warrant (Modified: WAWD 2-12-2020)

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the matter of the Search of	)	
	)	
Information Stored by Google	)	Case No. MJ23-275
	)	
	)	

APPLICATION FOR A GEOFENCE SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the person or property described in Attachment A, located in the Northern District of California, there is now concealed property and evidence described in Attachment B. This court has authority to issue this warrant under 18 U.S.C. §§ 2703(c)(1)(A) and 2711(3)(A).

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1343	Bank Fraud
18 U.S.C. § 1028A	Aggravated Identity Theft

The application is based on the facts set forth in the attached affidavit, which is incorporated herein by reference with all attachments and exhibits.

Pursuant to Fed. R. Crim. P. 41, this warrant is presented by:

☒ by reliable electronic means; or ☐ telephonically recorded

Natalie Leavitt

Applicant's signature

Natalie Leavitt, Special Agent

Printed name and title

☐ The foregoing affidavit was sworn before me and signed in my presence, or

☒ The above-named officer provided a sworn statement attesting to the truth or the foregoing affidavit by telephone/

Date: 6/2/2023 10:45 AM

Judge's signature

Hon. Brian A. Tsuchida, United States Magistrate Judge

Printed name and title

City and state: Seattle, Washington

USAO # [###]

STATE OF WASHINGTON)
) ss
COUNTY OF [COUNTY])

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A GEOFENCE SEARCH WARRANT

I, NATALIE LEAVITT, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AFFIANT BACKGROUND

1. I make this affidavit in support of an application for a warrant to search information that is stored at premises controlled by Google, an electronic communication service and remote computing service provider headquartered in Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government the information further described in Attachment B.I. The government will then review that information and seize the information that is further described in Attachment B.II.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been so employed since April 2022. I am currently assigned to the Bellingham Resident Agency of the Seattle Division. The FBI is responsible for enforcing the federal criminal statutes of the United States. While employed as an FBI Agent, I have investigated a wide array criminal violations including but not limited to assault, sexual abuse, and embezzlement and theft from Indian tribal organizations. Prior to working for the FBI, I spent over three years in the accounting industry working as an accountant in the financial reporting department for a private company. I am also a licensed Certified Public Accountant.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1344 (bank fraud) and 1028A (aggravated identity theft) have been committed by unknown persons. There is also probable cause to search the information described in Attachment A for evidence of these crimes described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by U.S.C. § 2711. Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

6. Based on my training and experience, I know that cellular devices, such as mobile telephone(s), are wireless devices that enable their users to send or receive wire and/or electronic communications using the networks provided by cellular service providers. Using cellular networks, users of many cellular devices can send and receive communications over the Internet.

7. I also know that many devices, including but not limited to cellular devices, have the ability to connect to wireless Internet ("wi-fi") access points if the user enables wi-fi connectivity. These devices can, in such cases, enable their users to send or receive wire and/or electronic communications via the wi-fi network. A tablet such as an iPad is an example of a device that may not have cellular service but that could connect to the Internet via wi-fi. Wi-fi access points, such as those created through the use of a router and offered in places like homes, hotels, airports, and coffee shops, are identified by a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

service set identifier ("SSID") that functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely scan their environment to determine what wi-fi access points are within range and will display the names of networks within range under the device's wi-fi settings.

8. Based on my training and experience, I also know that many devices, including many cellular and mobile devices, feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices, such as between a device such as a cellular phone or tablet and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by devices within the Bluetooth device's transmission range, to which it might connect.

9. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system ("GPS") technology. Using this technology, the device can determine its precise geographical coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the apps' operation.

10. Based on my training and experience, I know Google is a company that, among other things, offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Nearly every device using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

11. In addition, based on my training and experience, I know that Google offers numerous apps and online-based services, including messaging and calling (*e.g.,* Gmail, Hangouts, Duo, Voice), navigation (Maps), search engine (Google Search), and file creation, storage, and sharing (*e.g.*, Drive, Keep, Photos, and YouTube). Many of these

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

services are accessible only to users who have signed in to their Google accounts. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address (*e.g.*, example@gmail.com). Other services, such as Maps and YouTube, can be used with limited functionality without the user being signed in to a Google account.

12. Based on my training and experience, I also know Google offers an Internet browser known as Chrome that can be used on both computers and mobile devices. A user has the ability to sign-in to a Google account while using Chrome, which allows the user's bookmarks, browsing history, and other settings to be uploaded to Google and then synced across the various devices on which the subscriber may use the Chrome browsing software, although Chrome can also be used without signing into a Google account. Chrome is not limited to mobile devices running the Android operating system and can also be installed and used on Apple devices and Windows computers, among others.

13. Based on my training and experience, I know that, in the context of mobile devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, devices that do not run the Android operating system, such as Apple devices.

14. According to my training and experience, as well as open-source materials published by Google, I know that Google offers accountholders a service called "Location History," which authorizes Google, when certain prerequisites are satisfied, to collect and retain a record of the locations where Google calculated a device to be based on information transmitted to Google by the device. That Location History is stored on Google servers, and it is associated with the Google account that is associated with the device. Each accountholder may view their Location History and may delete all or part of it at any time.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

15. Based on my training and experience, I know that the location information collected by Google and stored within an account's Location History is derived from sources including GPS data and information about the wi-fi access points and Bluetooth beacons within range of the device. Google uses this information to calculate the device's estimated latitude and longitude, which varies in its accuracy depending on the source of the data. Google records the margin of error for its calculation as to the location of a device as a meter radius, referred to by Google as a "maps display radius," for each latitude and longitude point.

16. Based on open-source materials published by Google and my training and experience, I know that Location History is not turned on by default. A Google accountholder must opt-in to Location History and must enable location reporting with respect to each specific device and application on which they use their Google account in order for that usage to be recorded in Location History. A Google accountholder can also prevent additional Location History records from being created at any time by turning off the Location History setting for their Google account or by disabling location reporting for a particular device or Google application. When Location History is enabled, however, Google collects and retains location data for each device with Location Services enabled, associates it with the relevant Google account, and then uses this information for various purposes, including to tailor search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location-based advertising. As noted above, the Google accountholder also has the ability to view and, if desired, delete some or all Location History entries at any time by logging into their Google account or by enabling auto-deletion of their Location History records older than a set number of months.

17. Location data, such as the location data in the possession of Google in the form of its users' Location Histories, can assist in a criminal investigation in various

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ways. As relevant here, I know based on my training and experience that Google has the ability to determine, based on location data collected and retained via the use of Google products as described above, devices that were likely in a particular geographic area during a particular time frame and to determine which Google account(s) those devices are associated with. Among other things, this information can indicate that a Google accountholder was near a given location at a time relevant to the criminal investigation by showing that his/her device reported being there.

18. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provide clues to their identity, location, or illicit activities.

19. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (*i.e.,* session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

PROBABLE CAUSE

20. The following facts come from Key Bank's internal investigation file:

21. K.P. has a checking account and a Home Equity Line of Credit (HELOC) account with Key Bank. On May 21, 2021, K.P.'s purse was stolen. Inside the purse was K.P.'s driver's license and credit and debit cards.

22. On May 9, 2022, Key Bank's Orcas Island branch at 487 Main Street, Eastsound, Washington, received a call from phone number 682-816-2170, inquiring about the balance on K.P.'s checking account. A Key Bank representative responded that the amount in the checking account was around $26,000.

23. On May 18, 2022, at approximately 12:41 pm PST, an unknown individual (UNSUB) in a wig, surgical mask, and glasses entered Key Bank's Orcas Island branch. The UNSUB sought to withdraw $30,000 in cash from K.P.'s checking account. The UNSUB used K.P.'s driver's license and one of her debit cards as identification.

24. Adria Garcia, Key Bank's Orcas Island branch manager, informed the UNSUB that it would take time to withdraw that amount from the checking account in cash but that a check from the Home Equity Line of Credit (HELOC) account could be issued that same day.

25. The UNSUB requested a withdrawal of $800,000 from K.P.'s HELOC account, to be split into two checks: a $350,000 check made payable to Cory Logan and a $450,000 check made payable to Luis Perez.

26. Garcia did not follow the bank's policies in processing the withdrawal. For every bank transaction, a bank teller must run the customer's identification through Intellicheck, the identification verification system utilized by the bank. But Garcia did not

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

do so with the UNSUB's, or any other customer's, identification that day. To process withdrawals of this size, a system override is required, and the bank's upper management must approve the override. Instead of obtaining this approval, Garcia instructed her lead bank teller to effectuate the system override. Throughout her tenure at Key Bank, Garcia obtained management approval for a system override for large transactions. But she did not do so for this transaction.

27. At 12:54 pm PST, the UNSUB left the bank with the two checks.

28. At 4:15 pm PST that day, the $450,000 check was deposited at Chase Bank's Cordata branch at 4279 Guide Meridian Rd, Bellingham, WA. At 4:32 pm PST that day, the $350,000 check was deposited at Chase Bank's Barkley Village branch at 3110 Woburn St, Bellingham, WA.

29. Surveillance footage from Key Bank's Orcas Island branch captured a female in a blond wig, medical mask, and glasses inside the bank from 12:41 PST to 12:54 PST. During this time, this female had a phone with her, which is visible in the surveillance footage. See Exhibit 1.

30. Based on the foregoing, I submit that there is probable cause to search information that is currently in the possession of Google and that relates to the devices that reported being within the Target Locations described in Attachment A—namely, Key Bank Orcas Island branch, where the checks were withdrawn, and Chase Bank Cordata branch Chase Bank Barkley Village branch, where the checks were deposited—during the time period described in Attachment A for evidence of the crime(s) under the investigation. The information to be searched includes (1) identifiers of each device; (2) the location(s) reported by each device to Google and the associated timestamp; and (3) basic subscriber information for the google account(s) associated with each device.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

31. The proposed warrant sets forth a multi-step process whereby the government will obtain the information described above. Specifically, as described in Attachment B.I:

a. Using Location History data, Google will identify those devices that it calculated were or could have been (based on the associated margin of error for the estimated latitude/longitude point) within the Target Location described in Attachment A during the time period described in Attachment A. For each device, Google will provide a anonymized identifier, known as a Reverse Location Obfuscation Identifier ("RLOI"), that Google creates and assigns to device for purposes of responding to this search warrant; Google will also provide each device's location coordinates along with the associated timestamp(s), margin(s) of error for the coordinates (i.e,. "maps display radius"), and source(s) from which the location data was derived (e.g., GPS, wi-fi, bluetooth), if available. Google will not, in this step, provide the Google account identifiers (e.g., example@gmail.com) associated with the devices or basic subscriber information for those accounts to the government.

The government shall review the Device List and rule out any devices that are unlikely to be related to the investigation based on timing and location information, keeping in mind that the accuracy of location information that Google provides can vary from device to device and that it may not be possible to rule out a device based on timing and location information alone. For example, law enforcement may remove devices were moving through the Target Location(s) in a manner inconsistent with the facts of the underlying case, or for similar reasons appear not to be relevant to the investigation. After ruling out those devices (if any) that are unlikely to be related to the investigation, the government shall

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

identify to Google the devices about which it seeks to obtain Google account identifiers and basic subscriber information.

If additional location information for a given device ID is needed in order to determine whether that device is relevant to the investigation, law enforcement will request a further search warrant that will require Google to provide additional data for time period(s) and locations that fall outside of the Search Parameter(s).

Google will then disclose to the government the Google account identifier associated with the devices identified by the government, along with basic subscriber information for those accounts.

32. This process furthers efficiency and privacy by allowing for the possibility that the government, upon reviewing contextual information for all devices identified by Google, may be able to determine that one or more devices associated with a Google account (and the associated basic subscriber information) are likely to be of heightened evidentiary value and warrant further investigation before the records of other accounts in use in the area are disclosed to the government.

33. **The proposed warrant would not authorize the disclosure or seizure of any email communications or messages (SMS text or Google chat).**

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CONCLUSION

34. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c).

35. I further request that the Court direct Google to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectively submitted,

Natalie Leavitt

NATALIE LEAVITT
Special Agent, FBI

The above-named agent provided a sworn statement to the truth of the foregoing affidavit by telephone on 2 day of June, 2023.

BAT

HON. BRIAN A. TSUCHIDA
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

EXHIBIT 1
Surveillance Images of UNSUB

05/18/2022 12:43:44.39
Teller 2
Surveillance
WA372ORCASISLAND

This photographic image is generated for the internal use of KeyBank. KeyBank makes no representation or warranty of any kind with respect to this photograph, film, videotape, or digital image and specifically disclaims liability to any person or entities for all damages, losses, claims, or expenses (including attorney's fees) arising from the furnishing or subsequent use, distribution or publication of this image/video. Any use of this image/video by any party not employed directly by KeyBank is undertaken at the risk of and is the sole responsibility of the user.

05/18/2022 12:46:01.19
Teller 2
Surveillance
WA372ORCASISLAND

This photographic image is generated for the internal use of KeyBank. KeyBank makes no representation or warranty of any kind with respect to this photograph, film, videotape, or digital image and specifically disclaims liability to any person or entities for all damages, losses, claims, or expenses (including attorney's fees) arising from the furnishing or subsequent use, distribution or publication of this image/video. Any use of this image/video by any party not employed directly by KeyBank is undertaken at the risk of and is the sole responsibility of the user.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

Property To Be Searched

This warrant is directed to Google LLC, an electronic communication service and remote computing service provider headquartered in Mountain View, California, and applies to:

(1) Location History data, sourced from information including GPS data and information about visible wi-fi points and Bluetooth beacons transmitted from devices to Google, reflecting devices that Google calculated were or could have been (as indicated by margin of error, *i.e.,* "maps display radius") located within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below ("Initial Search Parameters"); and

(2) identifying information for Google Accounts associated with the responsive Location History data.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Initial Search Parameters

Search Parameter 1

- Date: 5/18/2022
- Time Period (including time zone): 12:36 pm – 12:59 pm pacific standard time
- Target Location: Geographical area identified below:

Point 1: 48.694999, -122.905018
Point 2: 48.695006, -122.904455
Point 3: 48.694648, -122.904479
Point 4: 48.694657, -122.905051

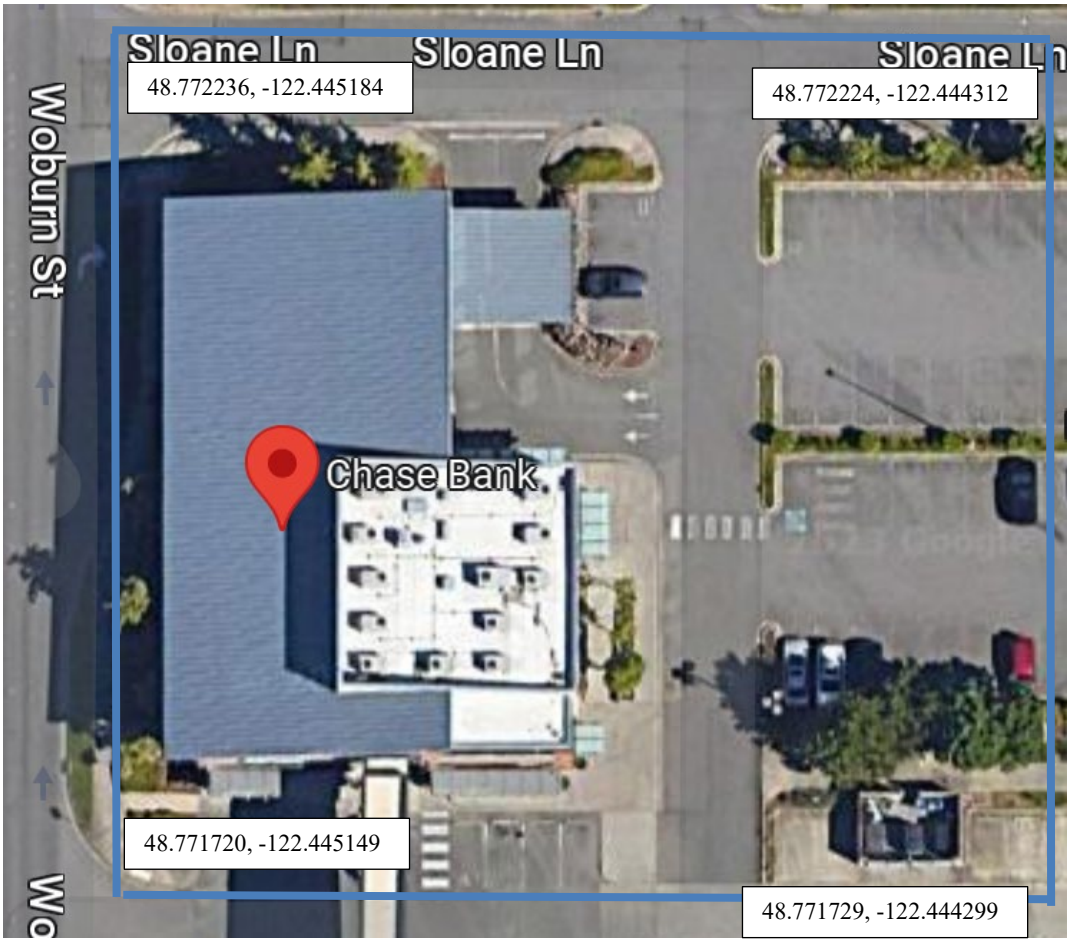
- Time Restriction: Devices that reported their location more than once within the Target Location on the date and during the time period above and where at least ten minutes elapsed between the time that the first time the device reported its location and the last time that the device reported its location.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Search Parameter 2

- Date: 5/18/2022
- Time Period (including time zone): 4:13 pm – 4:17 pm pacific standard time
- Target Location: Geographical area identified in the picture below:

Point 1: 48.772236, - 122.445184
Point 2: 48.772224, -122.444312
Point 3: 48.771729, -122.444299
Point 4: 48.771720, -122.445149



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Search Parameter 3

- Date: 5/18/2022
- Time Period (including time zone): 4:30 pm – 4:35 pm pacific standard time
- Target Location: Geographical area identified in the picture below:

Point 1: 48.796392, -122.486992
Point 2: 48.796390, -122.486300
Point 3: 48.795961, -122.486304
Point 4: 48.795953, -122.486979

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

Particular Items to Be Seized

I. Information to be disclosed by Google

The information described in Attachment A, via the following process:

1. Google shall query location history data based on the Initial Search Parameters specified in Attachment A. For each location point recorded within the Initial Search Parameters, and for each location point recorded outside the Initial Search Parameters where the margin of error (*i.e.*, "maps display radius") would permit the device to be located within the Initial Search Parameters, Google shall produce to the government information specifying the corresponding unique device ID, timestamp, location coordinates, display radius, and data source, if available (the "Device List").

2. The government shall review the Device List and rule out any devices that law enforcement believes are unlikely to be related to the investigation based on timing and location information, keeping in mind that the accuracy of location information that Google provides can vary from device to device and that it may not be possible to rule out a device based on timing and location information alone. For example, law enforcement may remove devices that were moving through the Target Location(s) in a manner inconsistent with the facts of the underlying case, or for similar reasons appear not to be relevant to the investigation. After ruling out those devices (if any) that law enforcement believe are unlikely to be related to the investigation, the government shall identify to Google the devices about which it seeks to obtain Google account identifier and basic subscriber information.

3. If additional location information for a given device ID is needed in order to determine whether that device is relevant to the investigation, law enforcement will request a

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

further search warrant that will require Google to provide additional data for time period(s) and locations that fall outside of the Initial Search Parameter(s).

4. Google shall disclose to the government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Accounts associated with each device ID appearing on the Device List that the government has identified.

This warrant does not authorize the disclosure or seizure of any email communications or messages (SMS text or Google chat).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

II. Information to Be Seized

All information described above in Section I that constitutes evidence of violations of Title 18, United States Code, Sections 1344 and 1028A have been committed on 5/18/22 involving unknown person(s).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google LLC. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google LLC, and they were made by Google LLC as a regular practice; and

b. such records were generated by Google LLC electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature